Information
and Privacy
Commissioner/
Ontario

The State of Privacy and Data Protection in Canada, the European Union, Japan and Australia

Ann Cavoukian, Ph.D.
Commissioner
June 2003

Information and Privacy Commissioner/Ontario

80 Bloor Street West
Suite 1700
Toronto, Ontario
M5S 2V1

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Web site: www.ipc.on.ca

Commissioner Ann Cavoukian gratefully acknowledges the assistance of Mary O'Donoghue, Legal Counsel, in the preparation of this paper.

This publication is also available on the IPC Web site.

103-07041/

Table of Contents

Introduction 1

Privacy in Canada 2

Privacy in the Private Sector – Federal Canada 2

Personal Information Protection and Electronic Documents Act (PIPEDA) 2

Findings of the Privacy Commissioner of Canada 2

Consent – Air Canada Frequent Flyer Plan Decision 3

Controlling Agents 4

Jurisdiction – Credit Reporting Agencies 4

Industry Canada and Representations on the Internet – Cross-Border 5

Other Privacy Developments 5

Police Video Surveillance in Public Places 5

Solicitor and Client Privilege 6

Police Search of Lawyers' Office 6

Solicitor-Client Confidentiality 8

Money Laundering Reporting and Solicitor and Client Privilege 8

Cross-Border Issues under the *Sarbanes-Oxley Act* 9

Privacy in the Private Sector – Provincial Developments 10

Ontario 10

Private Sector Privacy Bill 10

Release of Patient's Personal Records: A Wake-Up Call to All Companies .. 11

Ontario Commissioner Research Partnership with Privacy Think Tank 12

Private Sector Privacy – British Columbia and Alberta 12

Liability of Credit Reporting Agencies 14

Disclosure of Information in the Professional Context 14

Alberta Health Information 14

Ontario – Disclosure about Brokers 16

National Security 16
Annual Report to Parliament of the Privacy Commissioner of Canada 16
Ontario IPC Response 17
Other Support for the Privacy Commissioner 18
Government of Canada Lawful Access Proposal 18
Privacy Commissioners Oppose the Plan 19
Minister of Immigration Proposal for National ID Card 21
Canada Customs and Revenue Agency (CCRA) Travellers' Database 23
The Information to be Submitted on Each Individual 23
European Union 27
Video Surveillance Consultation 27
Passenger Name Record (PNR) Transmission to US Customs 27
Retention of Electronic Communications Traffic Data 29
Privacy in Japan 30
Privacy in Australia 31
Conclusion 32
Notes 33

Introduction

Privacy has not taken a back seat in public attention during the past year. National security and anti-terrorism initiatives by governments have continued to dominate the agenda for those concerned with privacy protection. The security developments have been a source of serious concern in many jurisdictions, including Canada, the US, the UK and the European Union. Major issues include the creation by governments of databases for the tracking of airline travellers. Under these programs, governments are collecting large amounts of sensitive personal information, keeping it for lengthy periods and using it for purposes that are unrelated to the war on terror. Other disturbing developments are proposals by governments in Canada, the UK and the Philippines to require citizens to obtain national ID cards, or to require ISPs to retain all customer electronic communications traffic information for possible use by law enforcement agencies.

In his case summaries, the Privacy Commissioner of Canada continues to provide guidance in his interpretation of the *Personal Information Protection and Electronic Documents Act* (PIPEDA). The corporate and commercial bar in Canada has followed the Commissioner's rulings with keen interest. The Canadian Bar Association has recently approved the creation of a national Privacy Law Section, which will work in conjunction with already established provincial bar association privacy sections in Ontario, Alberta and British Columbia.

Privacy Commissioners in Canada have been very active in making submissions responding to government initiatives that impact on privacy, especially in national security. Their efforts have met with considerable public support. There have been some successes where the government has responded positively to privacy concerns raised by the Commissioners. The most notable change was to the Canada Customs and Revenue Agency's database for tracking travellers, which moved from an all-inclusive model to one that is more targeted and nuanced.

Other developments of interest are in the area of solicitor and client privilege, especially where money laundering and corporate malfeasance reporting requirements apply to lawyers. Lawyers in Canada have been successful in the highest courts in arguments for a strong legal protection for solicitor and client privilege. This has persuaded the Government of Canada to exempt lawyers, at least for the moment, from requirements of reporting on their clients under money laundering legislation.

Finally, concern about the proliferation of video surveillance cameras in public places has triggered litigation on constitutional grounds in Canada, and a working paper to study protections for citizens in the European Union.

Privacy in Canada

Privacy in the Private Sector – Federal Canada

Personal Information Protection and Electronic Documents Act (PIPEDA)

The Government of Canada enacted legislation to protect the personal information of individuals that is held by private sector entities in the course of commercial activities.[1] The Act also protects the information of federally regulated employees. Excluded is personal information that is collected, used or disclosed by individuals for purely domestic and non-commercial purposes, and personal information that is collected, used or disclosed for journalistic, literary or artistic purposes.

The legislation came into force in 2001, and will apply to the private sector in stages. In its initial phase, the Act applies to federally regulated works, undertakings and businesses, notably banks, airlines, railways and broadcasting companies. The Act currently applies also to provincially regulated entities that disclose personal information across borders for consideration.

In 2004, PIPEDA will apply to provincially regulated entities that collect, use and disclose personal information in the course of commercial activities. The federal government is asserting jurisdiction over provincially regulated entities under the federal "trade and commerce power" and has thus limited the reach of the Act to commercial activities, leaving uncovered the non-commercial activities of non-profit entities and provincially regulated employee information.

The Privacy Commissioner of Canada, George Radwanski is the oversight body with responsibility for ensuring compliance with the Act. He is an independent Officer of Parliament, who also has jurisdiction with respect to public sector privacy regulation. The Commissioner is an ombudsman, who has extensive investigative powers and may make findings, issue reports and make recommendations. In addition, an aggrieved person may apply to the Federal Court for redress, including damages.

Findings of the Privacy Commissioner of Canada

To date, Commissioner Radwanski has issued more than 125 summary reports of his findings in individual complaints under PIPEDA.[2]

The following are some interesting reports issued by the Commissioner.

Consent – Air Canada Frequent Flyer Plan Decision

The consent of the individual is the key to the legislation. It must be obtained for the collection, use and disclosure of personal information, with some specified exceptions. The consent may be express or implied. While PIPEDA permits an organization to rely on implied consent, express consent is required for sensitive personal information. Consent must be informed, and this is required whether or not the consent is express or implied.

In a decision involving the Air Canada frequent flyer plan, Aeroplan, the Commissioner acknowledged that opt-out consent is contemplated by PIPEDA, but nevertheless narrowed the scope of situations where this approach would be valid. The Airline collects, uses and discloses the personal information of its frequent flyer plan members, and routinely discloses this information to other Air Canada divisions, to member airlines of the Star Alliance airline network as well as to other arms length business partners. This use and disclosure is not revealed to Plan members upon enrollment.

In June 2001, the airline sent a brochure entitled "All About Your Privacy" to 60,000 of its approximately 6 million Aeroplan members, and presented five scenarios for sharing the personal information with other parties, asking for consent to these disclosures on an opt-out basis. None of the companies to which it was proposed to make the disclosures was named. Unless a positive objection was registered, the Aeroplan member was assumed to have consented to the disclosure.

The Commissioner held that the brochure was vague, confusing and open-ended, and did not provide sufficient specific information, (including information about purposes), regarding the disclosures to permit informed consent. In regard to whether an opt-out form of consent was appropriate, he ruled that regard must be had to the sensitivity of the information and the reasonable expectations of the individual. Opt-out is the weakest form of consent and its scope of acceptable use should be limited.

The information being shared included financial information, information about personal or professional interests, demographics and preference for products, and this information was categorized as "sensitive personal information" by the Commissioner, and thus subject to a higher standard of positive opt-in consent.

The Commissioner found the following facts compelling: that the airline was already disclosing information in 3 of the 5 categories; and that it did not provide information about disclosure upon membership enrollment, and indeed intimated that it did not share information. He said that sending the brochure out to only 1% of members was token compliance only, and the Act does not provide for that.

The Commissioner made the following recommendations:

- Air Canada should inform all Aeroplan members as to the collection, use, and disclosure of their personal information.
- Air Canada should clearly explain to all Aeroplan members the purposes for the collection, use, and disclosure of their personal information. This is not done adequately in the current version of the "All about your privacy" brochure.
- Air Canada should seek positive (i.e., opt-in) consent from all Aeroplan members regarding all information-sharing situations outlined in the brochure.
- Air Canada should establish appropriate procedures for obtaining positive consent.
- Air Canada should execute appropriate agreements with all the direct-mailing houses it employs as agents to ensure that the personal information of Aeroplan members is protected in accordance with the Act.
- Air Canada should suspend all information-sharing activities in respect of the Aeroplan program until the Commissioner's other recommendations have been implemented. Air Canada must inform the Commissioner within 60 days of its plan of action to implement his recommendations.[3]

Controlling Agents

The Commissioner has held that an organization that is contracting out the processing of personal information to another company must take steps to ensure the confidentiality and security of the information, to the point of ensuring that sub-contractors are bound by confidentiality contracts.[4]

Jurisdiction – Credit Reporting Agencies

In a recently issued report, an individual complained that a credit reporting agency had not responded to his request for access to his personal credit history and that it had refused to amend the information in his credit report. The Commissioner ruled that he had jurisdiction to investigate the complaint, because although credit reporting agencies are provincially regulated, they disclose personal information to clients across borders for consideration. The Commissioner concluded that the first part of the complaint was well founded in that the agency had taken too long to respond. However, he found that the second part of the complaint was not well founded as the personal information in issue was accurate and therefore there was no requirement on the agency to amend it.[5]

This case raises issues under the transitional provisions regarding applicability to provincially-regulated entities:

> 30(1) This Part does not apply to any organization in respect of personal information that it collects, uses or discloses within a province whose legislature has the power to regulate the collection, use or disclosure of information, unless the organization does it in connection with the operation of a federal work, undertaking or business or the organization discloses the information outside the province for consideration.

As noted above, credit reporting agencies are provincially regulated, and in Ontario, at least, are governed by a statutory regime that provides for many similar consumer protections and remedies regarding collection, use and disclosure as those under PIPEDA. Nonetheless, the Privacy Commissioner assumed jurisdiction and investigated the matter.

Industry Canada and Representations on the Internet – Cross-Border

In February 2003, the Competition Bureau of Industry Canada published a document on the application of the *Competition Act* to representations made on the Internet.[6]

The document sets out the rules and offences for commerce, online or offline. It speaks of combinations of online and offline commerce, such as representations made in Web sites that encourage consumers to buy items in a store.

On the issue of jurisdiction, Industry Canada clearly states that the rules will apply to businesses outside of Canada, in order to protect Canadian consumers:

> The Bureau will assert Canadian jurisdiction over foreign entities to the fullest extent authorized by law whenever necessary to protect the Canadian market from misleading representations and deceptive marketing practices. The Bureau will also actively seek the assistance and co-operation of foreign agencies to address misleading representations and deceptive marketing practices having an effect on the Canadian market. Such co-operation is facilitated through agreements and arrangements at both the government and agency level.

Other Privacy Developments

Police Video Surveillance in Public Places

In June 2002, the Privacy Commissioner of Canada initiated a constitutional challenge in the Supreme Court of British Columbia regarding the practice of police video surveillance in public places. Hearings began on March 12, 2003. The Commissioner's action is against

the Solicitor General of Canada, who has overall authority over the Royal Canadian Mounted Police, a federal police force that provides contracted policing services in many provinces. The Commissioner argues that such surveillance is not only unconstitutional, but it also breaches the federal public sector *Privacy Act*. The federal government's response, so far, is to argue that the Commissioner lacks standing to bring the constitutional application.[7] On June 10, 2003, the BC Supreme Court ruled that the federal privacy commissioner did not have legal standing to bring his challenge and it was dismissed.

Solicitor and Client Privilege

Police Search of Lawyers' Office

The Supreme Court of Canada has held that the solicitor and client privilege is of such importance that it is a fundamental aspect of the Canadian system of justice. The privilege has been held to be an element of fundamental justice under s. 7 of the Canadian *Charter of Rights and Freedoms*. Accordingly, the privilege must be given a large and liberal meaning, and any statutory derogations from the privilege must be read restrictively. Any doubt as to the reach of a derogation should be resolved in favour of protecting the confidentiality.

"Solicitor-client privilege must be as close to absolute as possible to ensure public confidence and retain relevance. As such, it will only yield in certain clearly defined circumstances, and does not involve a balancing of interests on a case-by-case basis."[8]

In a recent case, the Court has found a *Criminal Code* provision permitting the search and seizure of documents located in a lawyer's office to be unconstitutional. The privilege belongs to the client, and the *Code* provision required that any privilege be asserted by the lawyer. Failure by the lawyer to assert the privilege would result in the privilege being lost to the client. This the Supreme Court found unacceptable.

In the case, materials were seized by the police from law offices pursuant to warrants. The procedures prescribed by s. 488.1 for the protection of materials possibly protected by solicitor-client privilege were followed and claims of solicitor-client privilege were made by the law firms on their clients' behalf.

The Court said:

> It is critical to emphasize here that all information protected by the solicitor-client privilege is out of reach for the state. It cannot be forcibly discovered or disclosed and it is inadmissible in court. It is the privilege of the client and the lawyer acts as a gatekeeper, ethically bound to protect the privileged information that belongs to his or her client. Therefore, any privileged information acquired by the state without the consent of the privilege holder is information that the state is not entitled to as a rule of fundamental justice.

Among the deficiencies the Court found in the *Code* procedures were that the privilege would be lost through the absence or inaction of the lawyer, and the name of the client must always be produced, even if sometimes itself subject to privilege. There is no requirement that the client be notified – the absence of notice is the first step in a series of consequences, which can be fatal to maintaining the confidentiality of privileged documents. The court was provided with no remedial discretion in the context of the *Criminal Code* scheme, and thus could not save the privilege.

Finally, some appellate courts took issue with the fact that, pursuant to s. 488.1(4)(b), the Attorney General may be allowed to inspect the documents where the judge is of the opinion that it would materially assist the court in determining the question of privilege. Several courts held that this subsection effectively nullifies solicitor-client privilege before it is even determined that such privilege exists. There was no necessity for the determination of privilege to be made by the Attorney General.

The Court articulated the following principles with respect to the search of lawyers' offices:

1. No search warrant can be issued with regards to documents that are known to be protected by solicitor-client privilege.

2. Before searching a law office, the investigative authorities must satisfy the issuing justice that there exists no other reasonable alternative to the search.

3. When allowing a law office to be searched, the issuing justice must be rigorously demanding so to afford maximum protection of solicitor-client confidentiality.

4. Except when the warrant specifically authorizes the immediate examination, copying and seizure of an identified document, all documents in possession of a lawyer must be sealed before being examined or removed from the lawyer's possession.

5. Every effort must be made to contact the lawyer and the client at the time of the execution of the search warrant. Where the lawyer or the client cannot be contacted, a representative of the Bar should be allowed to oversee the sealing and seizure of documents.

6. The investigative officer executing the warrant should report to the Justice of the Peace the efforts made to contact all potential privilege holders, who should then be given a reasonable opportunity to assert a claim of privilege and, if that claim is contested, to have the issue judicially decided.

7. If notification of potential privilege holders is not possible, the lawyer who had custody of the documents seized, or another lawyer appointed either by the Law Society or by the court, should examine the documents to determine whether a claim of privilege should be asserted, and should be given a reasonable opportunity to do so.

8. The Attorney General may make submissions on the issue of privilege, but should not be permitted to inspect the documents beforehand. The prosecuting authority can only inspect the documents if and when it is determined by a judge that the documents are not privileged.

9. Where sealed documents are found not to be privileged, they may be used in the normal course of the investigation.

10. Where documents are found to be privileged, they are to be returned immediately to the holder of the privilege, or to a person designated by the court.[9]

The federal Department of Justice is currently drafting amendments to the *Criminal Code* to bring the provisions for the search of lawyers' offices into conformance with the Court's ruling.

Solicitor-Client Confidentiality

The Charter of Human Rights and Freedoms of Quebec contains explicit protection for privacy. In addition, the Civil Code protects privacy, as do separate Quebec statutes protecting privacy in both the public and private sectors. Recently, the Supreme Court of Canada granted leave to appeal a decision of the Quebec Court of Appeal regarding the confluence between solicitor and client privilege (in French "secret professionnel de l'avocat") and the right to privacy under the *Charter*. Section 9 of the Quebec Charter of Rights and Freedoms gives the "secret professionnel de l'avocat" the status of a fundamental human right, and the Court will consider whether this should receive broad and generous interpretation or a restrictive one.[10]

Money Laundering Reporting and Solicitor and Client Privilege

The Government of Canada passed anti-terror financing and money laundering legislation, requiring a variety of persons to report to government on "suspicious" transactions of their clients.[11] Included were the legal profession. Lawyers had forcefully lobbied the Minister of Justice to omit lawyers from the reporting requirements, on the grounds that the statutory requirement derogated from solicitor and client privilege, failed to recognize the unique nature of lawyer-client confidentiality, and would destroy the lawyers' confidential relationship with their clients. The Minister refused to consider an exemption for lawyers.

The Canadian Bar Association and the Federation of the Law Societies of Canada[12] (the FLSC) initiated litigation against the legislative inclusion of lawyers. The government forced the litigants to bring a separate action in each province. In the first application brought in British Columbia, the court issued a stay of the lawyers' reporting requirement, suspending

the application of the contested provisions for BC lawyers. Following similar results in Alberta, Ontario, Nova Scotia and Saskatchewan, the FLSC and the Attorney General of Canada signed a agreement in May 2002 that temporarily exempted all lawyers in Canada, including Quebec notaries, pending an appeal in the BC courts.

In March 2003, the Government announced that it would exempt lawyers from requirements under the money laundering legislation to divulge confidential communications with their clients.

At the same time, the government has announced its intention to introduce "re-designed" rules regarding lawyers, promising that they will not adversely affect legal counsels' ability to fulfill their duties and obligations to their clients, and that the "re-design" will take place in consultation with the legal profession.[13]

Cross-Border Issues under the Sarbanes-Oxley Act

The reach of the proposed reporting requirements to the US Securities and Exchange Commission under the *Sarbanes-Oxley Act* has cross-border affect, in that Canadian lawyers would be obliged to follow the rules in the same way as American lawyers. The rules affect lawyers appearing and practising before the SEC, as well as those even peripherally involved, foreign lawyers – including Canadians – in-house counsel and lawyers who hold non-legal positions, such as CEOs.

The Canadian Bar Association (the CBA) has declared that new rules would cast a chill on lawyer-client confidentiality and threaten confidence in international capital markets.

The "noisy withdrawal" rule is the most contentions, and in the view of the CBA, has the effect of turning "trusted counsellors into securities police." The rule requires lawyers to blow the whistle on a client if they suspect any violation of the US securities law. Lawyers would be required to report up the corporate ladder – potentially as high as the board of directors – any misconduct or violation they "reasonably believe" may be contained in documents submitted to the SEC.

The CBA filed a formal submission with the SEC, and objected to the rule on the basis that it is a dramatic departure from solicitor and client privilege would seriously erode the lawyer and client relationship and threaten the independence of the legal profession. The rule would breach the lawyers' ethical obligations to their clients. Clients would be very reluctant to obtain advice from their lawyers, which would "interfere with the positive role lawyers have always played in assisting their clients to come to capital markets in a forthright, reliable and honest way."

On the question of the independence of the bar, the CBA stated that the attempt of a US administrative body such as the SEC to discipline Canadian lawyers would interfere with the self-governance of the Canadian bar, which is already subject to appropriate professional rules of conduct.

The CBA recommended that the rules be applied only to lawyers practicing in the US, or that they recognize that Canadian ethical standards for lawyers are comparable and acceptable and do not require supplementation. The CBA further recommended that the rule be limited to lawyers directly involved in SEC filings.[14]

In January 2003, the SEC proposed a modification of the rule, and asked for comments. Lawyers would still be required to report misconduct or fraud up the corporate ladder to audit committees or the full board of directors. However, if lawyers withdraw their services, the client would have the obligation of reporting the lawyer's withdrawal to the SEC.[15]

The CBA said that the changes were a positive step, however, they did not go far enough, and the association submitted further comments on the changed rules on March 20, arguing that the rule still violates the privilege, and inhibits lawyer/client communication.[16]

Privacy in the Private Sector – Provincial Developments

Ontario

Private Sector Privacy Bill

In February 2002, the Government of Ontario released a draft private sector privacy bill for public consultation – the draft *Privacy of Personal Information Act* (PPIA). Over 600 submissions were received by the Ministry of Consumer and Business Services from many sectors, and consultations with stakeholders continued through the summer. The Ministry made many amendments to the draft bill, refining it in response to the issues raised by stakeholders. The draft went to Cabinet in the fall, but was not introduced as a bill prior to the Legislature rising in December 2002.

The Information and Privacy Commissioner of Ontario wrote an open letter to the Premier of Ontario, voicing her disappointment at the failure of the Government to introduce the bill. She said:

> With the current session of the Ontario Legislature having concluded last week, it is clear that the Ontario Government has decided not to fulfill its commitment to introduce "made in Ontario" health and private sector privacy legislation. This is a significant loss to the people of Ontario, and I am deeply disappointed with this failure to take action.

She said that the legislation was ready to go and there was clear public support. The Ministry had consulted extensively and resolved many of the key issues. Without legislation, entire sectors of society will remain without legislated protections. This has the potential to have a long-term adverse effect as Ontario lags behind other provinces' and countries' privacy protection.

The proposed legislation provided coverage for the protection of health care information. It is the Commissioner's view that health privacy legislation is critical for the development of electronic patient records, dedicated health networks, and the use of genetic test information. The absence of legislative protections deters the adoption of new information technology in health sector. Inconsistent health privacy rules will pose a barrier to initiatives such as the integrated delivery of health care services, primary care reform and the advancement of electronic health records.[17]

The Premier of Ontario responded. He noted that he appreciated the Commissioner's candour on this important issue. His government shares the view that the privacy and health information of Ontario residents must be protected and that there is no doubt that privacy is a fundamental right. He agreed that action must be taken to guarantee the security of personal information including medical records. However, he said that there were still some outstanding concerns with stakeholders to address. He did not believe that the opportunity to introduce privacy legislation before the application of PIPEDA was lost – there was sufficient time to introduce privacy legislation in a future session of the Legislature before January 2004. He said that the responsible Ministry would continue to address the remaining stakeholder concerns.

The government reconvened the Legislature on April 30, 2003. As of the time of writing, no legislation had been introduced.

Release of Patient's Personal Records: A Wake-Up Call to All Companies

An incident that highlighted the necessity for formal rules governing the handling of personal health information occurred in February 2003. An inadvertent disclosure of sensitive medical records resulted in information about an identified patient appearing on the back of real estate flyers distributed to a number of Toronto-area homes. Commissioner Cavoukian called the incident a "wake-up call for all companies:"

> If I were on the board of directors of any firm and heard this type of story, I would immediately call my CEO and ask, 'Are we at risk? What procedures do we have in place?'... Every company must have strong privacy and security policies in place – written policies that have been clearly communicated to all staff. Personal information should never just be thrown out in the trash or put out for recycling.

> Every company must have a standard operating procedure for the secure disposal and destruction of personal records – a procedure that does not allow for the records to be restored.

She said that senior officers at every company today should be demanding answers on what happens to personal information at their company. Each company should assign one individual to be responsible and accountable for the retention and disposal of all personal records, and to ensure that the necessary sign-offs have been obtained. Audit trails are also essential.[18]

Ontario Commissioner Research Partnership with Privacy Think Tank

In her continuing work with the private sector in encouraging good privacy practices in business, the Information and Privacy Commissioner and an Arizona-based "think tank" announced a joint research project that will compare the privacy practices of companies that operate in both Canada and the US.

The project will examine how the personal information of clients in Canada is handled compared to how the US operations of the same companies treat the personal information of American clients.

"It is very important to understand how global companies are responding to consumers' growing concerns about how their personal information is being managed," said the Commissioner. "In turn, companies will benefit from learning how their privacy programs compare to other organizations and what they need to do in order to build trust and minimize the possibility of a privacy breach."

The joint research program will be undertaken with the Ponemon Institute, a "think tank" focused on advancing responsible information and privacy management practices for business and government, on a global basis.

A group of leading Canadian and US commercial organizations representing a cross-section of industries will be invited to participate in the study. The project will cover a wide range of privacy issues, including privacy policies, training, privacy security methods, compliance and global standards. The study is expected to be completed in the summer of 2003 and survey results will be published on the IPC and Ponemon Institute Web sites.[19]

Private Sector Privacy – British Columbia and Alberta

In June 2002, the Government of British Columbia issued a paper on the topic of private sector privacy legislation for the province, and invited comments by the public. The government set out its general assumptions in the paper:

1. Given the January 1, 2004 "deadline" presented by the PIPED Act, each jurisdiction will need to develop its own legislation, challenge the federal legislation's proposed coverage in the courts, and/or prepare for coverage by the PIPED Act.

2. A "patchwork" of privacy regimes across the country will not be supported by the business sector, government, or privacy advocates. This does not mean that all jurisdictions must exactly duplicate the PIPED Act (with its formal incorporation of the CSA Model Privacy Code). Instead, it emphasizes the importance of a harmonized legislative framework and attention to a national minimum standard.

3. The PIPED Act has set the minimum standard of privacy protection in the private sector. Not only has it set precedent (one that is recognized by the European Union) but, if a provincial statute does not meet the PIPED standard, the federal government can choose not to recognize a provincial statute as "substantially similar."

4. A high percentage of Canadians are concerned about the protection of their personal information in the private sector and most private sector organizations are willing to comply with reasonable standards/requirements.

5. The consensus amongst business, interest groups and government leading to the development of the CSA Model Privacy Code and the passage of the PIPED Act supports this assumption.

6. Provincial private sector privacy legislation should strike a balance – ensuring comprehensive and harmonized protection of personal information in the private sector **and** allowing the private sector to collect, use and disclose the personal information it requires for appropriate business purposes. Any proposed legislation should also be reasonable for the private sector to implement and administer.

A private sector privacy act should be compatible with the provisions of the existing public sector act – the *Freedom of Information and Protection of Privacy Act* (FOIPP Act). The FOIPP has provided comprehensive privacy protection requirements for the public sector since 1993 (including the health sector) and is generally recognized as one of the strongest privacy regimes in Canada. Its provisions are laid out in a logical manner and are followed by an increasing number of private sector organizations involved in service delivery or other contractual partnerships with government. It provides a standard against which to measure and a model of legislative approach against which to compare.

The consultation paper requested public input on such questions as privacy codes as a foundation for compliance; whether opinions about other individuals are the personal information of that individual or of the subject of the opinion; should there be a frivolous and vexatious clause; and solutions to correction of information requests.[20]

During the winter of 2002/2003, it was reported that the Government of British Columbia was working on a draft bill in collaboration with the Government of Alberta, in order to ensure that they would be in harmony, thereby ameliorating cross-jurisdictional compliance problems. Strong rumours circulated that a bill would be introduced in late March. However, at the time of writing, no private sector privacy bill has been introduced in either province.

Liability of Credit Reporting Agencies

The Ontario Court of Appeal has recently issued a decision permitting a class action in tort to go ahead against two credit reporting agencies, Equifax and TransUnion, for damages resulting from improper consumer reporting. The case is a class action by a number of consumers who have claimed that they have been harmed by inaccurate credit reports circulated by Equifax and TransUnion. The motions judge had dismissed the case on the basis of three theories of liability: breach of fiduciary duty, invasion of privacy and negligence.

On appeal, only negligence, the third basis for liability was argued. The Court of Appeal decided that the two part test for negligence was made out: 1) there was proximity in the relationship between the consumer and the credit reporting agency so that harm from negligent reporting was reasonably foreseeable – there was a duty of care to the consumer; and 2) the Court did not accept that there were policy concerns that prima facie should result in no duty of care being found – specifically, it did not accept that there would be indeterminate liability to an indeterminate number of people for an indefinite period of time.

The Court did not decide the issue of liability (this will be left to trial) but merely decided whether there was a cause of action known to law – it decided that the cause of action was analogous to negligent misrepresentation. It also left to the trial court to decide whether the case was suitable to proceed as a class action and whether the statutory remedy under the *Consumer Reporting Act* is effective. It struck out the action against the US parents of the defendant Equifax and TransUnion. On the question of the availability of alternative legal remedies under the *Consumer Reporting Act* (Ontario), the Court was somewhat doubtful as to their efficacy, particularly since damages for harm suffered is not part of the legislative scheme.[21]

Disclosure of Information in the Professional Context

Alberta Health Information

The Information and Privacy Commissioner of Alberta has ordered pharmacists in Alberta not to disclose health services provider information to IMS HEALTH, Canada ("IMS").

The issue in this inquiry was whether information about the prescribing practices of doctors could be disclosed by pharmacists to IMS Canada under Alberta law, without the consent of the doctors.

The Commissioner held a public hearing under the *Health Information Act* (the HIA). He found that Alberta pharmacists and pharmacies were disclosing to IMS up to 37 data elements that pertained to prescribing activity.

The Commissioner held that:

1. Prescribing falls within a "health service" under the HIA, where it is included in the professional advice provided to an individual during a visit, and the professional advice is paid for directly and fully by the Department of Health;

2. A prescriber who is paid by the Department for a visit in which the prescriber gives professional advice, which includes prescribing, is providing a "health service" and is a "health services provider" for the purposes of the HIA;

3. The first and last name of such a health services provider is "health services provider information" under the HIA;

4. Disclosure of the first and last name of the health services provider in the context of the 35 other data elements disclosed to IMS would reveal "other information" about the health services provider within the meaning of section 37(2)(a) of the HIA;

5. The disclosure of the provider's first and last name in the context of other 35 data elements is prohibited under the HIA, unless the consent of the health services provider is obtained prior to the disclosure as per section 34 of the HIA.

The Commissioner ordered Alberta pharmacists and pharmacies not to disclose to IMS a health services provider's first and last name in the context of the 35 other data elements, unless that health services provider's consent was obtained as stipulated under the Act.[22]

This decision is in contrast to a report of the Privacy Commissioner of Canada, in the context of a complaint under PIPEDA (see above) about the disclosure of prescribing information by pharmacists without physician consent. The Commissioner held that the prescribing information was not the personal information of the physician under PIPEDA, but was "work product information."[23] His determination has been appealed to the Federal Court, Trial Division, and the litigation is ongoing.

It is important to note that the two Commissioners were interpreting quite different statutes.

Ontario – Disclosure about Brokers

The Superior Court of Ontario has ruled that brokerage firms have a duty to inform clients when their investment advisor has been disciplined for misconduct. Gordon J. ruled that Midland Walwyn Capital and Levesque Securities Inc. were negligent when they failed to advise a Waterloo couple about the history of their financial advisor, George Georgiou who had been fired for misconduct and was under investigation by the Toronto Stock Exchange. "The investor now can make a decision, if not with full knowledge, at least with better knowledge of who he is dealing with." Disclosure must be made even to clients not affected by losses. The brokerage firms, along with the financial advisor, were ordered to pay damages.[24]

National Security

National security issues continued to dominate the privacy arena in Canada during 2002/2003.

In the latter part of 2002 the Government of Canada continued to introduce legislative and administrative measures to address national security and the anti-terrorism issues. Many of these initiatives were very far-reaching in their effect on individual privacy and national attention has been focused on this aspect. The measures are not confined to anti-terrorism activity by government, but extend also to general criminal law investigations. The measures already in place include the issuance of new identity cards to be used on entry to Canada by all permanent residents, the collection of extensive personal information on travellers into Canada, and the retention of this information for a period of six years by the Canada Customs and Revenue Agency. Two controversial proposals were also made: a proposal for new law enforcement investigative powers in the cyber realm without judicial authorization ("lawful access"), and a proposal by the Minister of Citizenship and Immigration for the issuance of National ID cards to all Canadians, citizens and permanent residents.

The federal and provincial privacy commissioners have issued strong statements on the effect and reach of these measures.

Annual Report to Parliament of the Privacy Commissioner of Canada

On January 29, 2003, in his annual report to Parliament, the Privacy Commissioner of Canada issued unprecedented warnings in extremely strong language, as to the state of privacy in Canada. He said:

> It is my duty, in this Annual Report, to present a solemn and urgent warning to every Member of Parliament and Senator, and indeed to every Canadian:
>
> The fundamental human right of privacy in Canada is under assault as never before. Unless the Government of Canada is quickly dissuaded from its present course by Parliamentary action and public insistence, we are on a path that may well lead to the permanent loss not only of privacy rights that we take for granted but also of important elements of freedom as we now know it.

He said that the government of Canada was using the post-September anti-terrorism concerns as an excuse "for new collections and uses of personal information about all of us Canadians that cannot be justified by the requirements of anti-terrorism and that, indeed, have no place in a free and democratic society." The government had been unresponsive to the concerns expressed by him and other citizens, and gave as examples "Canada Customs and Revenue Agency's new "Big Brother" passenger database; the provisions of section 4.82 of Bill C-17; dramatically enhanced state powers to monitor our communications, as set out in the "Lawful Access" consultation paper; a national ID card with biometric identifiers, as advanced by Citizenship and Immigration Minister Denis Coderre; and the Government's support of precedent-setting video surveillance of public streets by the RCMP."

He was most concerned that the Government had chosen to ignore privacy concerns, and was "inappropriately willing to brush aside all criticisms."

Refusing to respond to the concerns raised by his office was a departure from a 20-year tradition, whereby the Government would normally pay heed to issues raised by the Privacy Commissioner of Canada.[25]

Ontario IPC Response

The Office of the Information and Privacy Commissioner/Ontario responded to the release of the federal Privacy Commissioner's annual report, stressing continuing concern over the federal government's extension of anti-terrorism measures to other, non-terrorist purposes. We said that we have serious concerns that an array of privacy-eroding legislation, intended to fight the threats of terrorism, will be used for purposes that have no connection to terrorism whatsoever. We expressed strong support for Commissioner Radwanski and his dogged efforts to bring national attention to a range of serious privacy issues facing the Canadian public. We said: "Privacy is a cherished value that goes to the essence of our everyday life, and we, as Privacy Commissioners, must stand together and do whatever we can to ensure that any diminishing of privacy is tied directly to real and measurable improvements in public safety and security."[26]

Other Support for the Privacy Commissioner

The International Civil Liberties Monitoring Group (ICLMG) also expressed written support for the Commissioner's message in his annual report. This is a national coalition set up to monitor the application of Canada's anti-terrorism legislation. The ICLMG shares the concerns expressed by the Commissioner that the privacy rights guaranteed by the Canadian Charters of Rights are being seriously eroded by the web of anti-terrorism legislation adopted by Parliament since September 2001, or about to be adopted in coming months.[27]

Other groups writing in support of the Commissioner's message were the Canadian Labour Congress and the Commonwealth Centre for Electronic Governance.

Government of Canada Lawful Access Proposal

The Canadian Government issued a draft discussion paper on August 25, 2002, on a plan to give law enforcement agencies more powers in carrying out electronic surveillance. It defined lawful access as the "lawful interception of communications, and the search and seizure of information by law enforcement and national security agencies."[28]

The proposal would amend the *Criminal Code* and other statutes. Because more communications take place in electronic form, the government argued that new laws with greater powers for the enforcement agencies are necessary in the fight against terrorism, and in normal criminal law enforcement investigations. The government also said that such laws are also necessary to meet its obligations under the Council of Europe Cyber Crime Treaty.

The proposed law would outlaw the possession of computer viruses, authorize police to order Internet providers to retain logs of all Web browsing for up to six months, and permit police to obtain a search warrant allowing them to find "hidden electronic and digital devices" that a suspect might be concealing. In most circumstances, a court order would be required for government agents to conduct Internet monitoring.

The discussion paper states: "It is proposed that all service providers (wireless, wireline and Internet) be required to ensure that their systems have the technical capability to provide lawful access to law enforcement and national security agencies." The Canadian Association of Chiefs of Police recommends "the establishment of a national database" with personal information about all Canadian Internet users. "The implementation of such a database would presuppose that service providers are compelled to provide accurate and current information," the draft says.

The proposal includes a data preservation model. One objective is to give investigators the ability to quickly preserve data sitting on an ISP's servers.

Today, ISPs can delete data as they see fit. For law enforcement to gain access to stored data, they require a search warrant or interception order. By the time they get it, the data could be gone. A preservation order requires judicial authorization, but with a lower threshold. A warrant would be required for access to the content of the stored information.[29]

Submissions on the proposal were received until December 16, 2002, the government having extended the date from November 15. The government also hosted meetings in Vancouver, Montreal and Ottawa with groups including NGOs and civil rights advocates. The meetings were well attended, and the government states that it received over 300 submissions on the proposal. A summary of submissions will be released by the Department of Justice.

Some of the criticisms of the proposal focused on the vast amounts of personal information that would be collected. "The new interception tools that ISPs and telecommunications companies would have to install on their networks would provide law enforcement agencies with the opportunity to collect vast amounts of content information that it would not be able to collect under any circumstances in the offline world," EPIC said in written comments. "Law enforcement authorities can hardly justify why they need to be able to collect all online content information while they cannot do it for regular mail."

Many of the submissions noted that the proposals were too vague and lacking in detail to be properly assessed.

Privacy Commissioners Oppose the Plan

A number of Privacy Commissioners, including our office, made submissions generally opposing the proposals.

The Ontario IPC submissions focused on the lack of oversight in the proposal:

> I suggest that broad judicial or other oversight mechanisms be built into the lawful access proposal to ensure public accountability, transparency and scrutiny. This oversight body should require routine reporting on measures undertaken in the name of law enforcement and an accounting of the efficacy of these measures. This reporting requirement should enhance public confidence.

Our office recommended that a determination must first be made as to whether new powers being introduced were actually necessary, or whether a full deployment of existing investigative tools, already available to law enforcement and intelligence agencies, would suffice. If extended powers are indeed believed to be necessary, then we must ensure that they are used and deployed in a manner consistent with specific law enforcement objectives. The power to deploy new methods of surveillance must only be used to meet legitimate law enforcement goals. The information collected through these powers must only be used for

identified law enforcement purposes and not for other purposes unrelated to public safety. Further, there is also a responsibility on the part of law enforcement officials, as counter-intuitive as it may sound, to protect the confidentiality of that information, particularly if it proves to have no relevance to law enforcement.

We said that mandating that Internet Service Providers (ISPs) track all online activities of their clients, so that this information could potentially be used for evidentiary purposes, would require a massive investment in storage capacity for all ISPs. Many of them would face significant business repercussions and/or cause them to raise fees substantially, impeding the penetration of online services in our society. This could well result in industry consolidation that would have negative implications for privacy and free speech as well as the overall growth and development of the Internet as a communications medium.[30]

The Information and Privacy Commissioner of British Columbia said that:

- No evidence has been offered that existing interception and search and seizure laws are inadequate for dealing with electronic communications. Nor does the Cyber-Crime Convention offer a persuasive rationale for the proposals.

- Privacy is a constitutionally protected right. Privacy in electronic communications should give way to law enforcement and national security needs only where those needs clearly outweigh the privacy interest and then only to the minimal extent necessary. There is clearly a reasonable expectation of privacy in e-mail. Existing standards respecting interception of private communications should apply to e-mail interception.

- Requiring service providers to acquire the technical capacity to provide lawful access inappropriately co-opts the private sector in state surveillance. The costs to service providers will raise consumer costs and may diminish the competitiveness of the Canadian Internet industry, thus exacerbating concerns about private sector involvement in state surveillance. The development and implementation of Internet technology will be driven by the interests of surveillance and not the needs or realities of Canadian businesses and consumers.

- A specific production order for telecommunications associated data should be available only from a judicial authority applying existing standards and not lower thresholds. Production orders for subscriber or service provider information also should only be available from a judicial authority applying existing standards.

- A data preservation order should be available only from a judicial authority using existing interception standards. Law enforcement authorities should, consistent with s. 487.11 of the *Criminal Code*, only be able to secure preservation when it would be impracticable to obtain a judicial order in the circumstances.

- In the context of creation of a number of surveillance databases in Canada, the proposal of the Canadian Association of Chiefs of Police to create a mandatory reporting database of all subscribers is worrisome. Final comment is withheld, however, pending further clarification of the proposal and its details.

- Independent oversight of the nature and frequency of use of any new lawful access powers is necessary, recognizing that such oversight must be designed to appropriately protect law enforcement interests.[31]

The proposal was also criticized by the Canadian Association of Internet Providers (CAIP). Jay Thompson, president of CAIP says that the government's proposals are unfair to Internet Service providers. The data retention requirement to retain customer information for lengthy periods is a serious concern.

Minister of Immigration Proposal for National ID Card

In November 2002, the Minister of Citizenship and Immigration suggested that each Canadian be issued special high-tech national identification cards for crossing the border into the United States. The card would be above and beyond existing ID such as passports and driver's licences and should be a requirement for entering and leaving Canada. The Minister said the cards would include photos but would not say whether they would include fingerprints or other biometrics. He said that should be part of the debate. The new card would replace the citizenship certificate card, which the government issues to new citizens and which displays a photograph and a signature but does not have high-tech security features. Privacy concerns would be addressed by only allowing biometrics to be used to match people to their cards, as opposed to compiling large databases of personal information, he said.

Minister Coderre was of the view that such a card would make it harder for would-be terrorists to obtain a fraudulent version and might be a way of persuading the US not to require visas for Canadians.

This suggestion was categorically opposed by Revenue Minister Caplan. She said it "isn't appropriate" to go down that road because of the potential threat to personal privacy a national ID card system would pose.

Nonetheless, Minister Coderre stated on November 18 that the matter was "still on the table," that the government had made no decision on the matter, and that there should be public debate. He referred the matter to the Parliamentary Committee on Citizenship and Immigration. The Committee held hearings during February and March 2003, receiving both oral and written submissions, and has not yet reported.

The Privacy Commissioner of Canada in his oral submissions to the Committee said that there is no need for a national identity card scheme in Canada and no justification for it. Such a card would be enormously damaging to privacy rights and totally foreign to Canadian traditions and values. The card was without support – 61 written submissions had been received by the Committee, and only 5 were in support of the idea. The Commissioner said that it was his duty to oppose a card because:

- A national identification card would radically change Canadian society by drastically infringing on the right to anonymity that is a key part of our fundamental right of privacy.

- In Canada, agents of the state have no right to require us to identify ourselves in our day-to-day lives unless we are being arrested or we are carrying out a licensed activity such as driving. The police cannot stop people on the street and demand, "Your papers, please." The creation of a de facto internal passport would inevitably change that.

- The creation of a biometric national identity card, which would be required for more and more purposes, would also open the door to relentless tracking of our activities, transactions and whereabouts.

- There is no realistic possibility that such a card could remain voluntary.

The Commissioner said that any such scheme must meet a four-part test of necessity, effectiveness, proportionality and lack of any less privacy-invasive alternative. In his view, a biometric card scheme fails on all of these bases. He urged the Committee to reject the notion.[32]

The Ontario IPC made a written submission to the Committee on the card. We said that such a card is completely unwarranted and will not achieve the principal goal of preventing terrorism or increasing public safety and security. In order to consider any possible introduction of a Canada-wide ID card system, a strong business and policy case must be made for it. One must demonstrate that it is not only necessary and effective, but that it also fits within the general constitutional nature of Canada and the accepted conventions of our civil society.

We said that we had concerns about the scope and proposed uses of the card and its potential effectiveness. Canada already has in place tools to meet concerns about fraud, money laundering, border protection and immigration, provision of government services and identity authentication. We had concerns about the card as a privacy-eroding tool. It would likely be supported by a national ID database or linked database registration system. The creation of a national database containing information on all Canadians would be unprecedented and far-reaching. The opportunity for government surveillance and tracking of lawful activities would be significantly expanded. Government promises could be broken

as to the narrowness of its use. To date we have not seen a justification for the introduction of such a measure.

Canada Customs and Revenue Agency (CCRA) Travellers' Database

Section 107(3) of the *Customs Act*[33] was amended in October 2002 to provide authority for the collection of extensive information about passengers flying into Canada under the CCRA Advanced Passenger Information (API) and Personal Name Record (PNR) programs.[34] All commercial air carriers and charters carrying persons into Canada and travel agents, and operators of reservations systems are required to submit specific information in the manifest.

The Information to be Submitted on Each Individual

- Surname, first name, middle name
- Date of birth
- Gender
- Citizenship or nationality
- Type of travel document that identifies them; country in which issued; document number
- Reservation locator number or status as crew member
- The information relating to the person in the reservation system[35]

All the above information becomes "customs information" under the Act and is to be provided in the manifest at time of departure. Access must be granted to the airlines' reservation information system. (s. 4) All other modes of transport into Canada may be covered by subsequent customs notice. (s. 8)

The use and disclosure of this information that is permitted is extensive.

> An official may use customs information for the purposes of administering or enforcing this Act, the *Customs Tariff*, the *Special Imports Measures Act* or Part 2 of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* of for any purpose set out in subsection (4), (5) or (7). (s. 107(3) of the *Customs Act*)

The purposes and uses set out include, (in addition to those set out above) criminal investigations and proceedings; tax and duty collection both federal and provincial; administration and enforcement, and policy development relating to federal programs such

as the Canada Pension Plan, Employment Insurance and *Immigration Act*; federal employee discipline; and the enforcement of various statutes by the RCMP (federal police force) and for various prescribed (but as yet unspecified) purposes.

In earlier discussion with the Privacy Commissioner of Canada, the CCRA had indicated that the personal information would be kept for a relatively short time, and then destroyed, unless it was to be used. However, when the legislation came into effect, the CCRA announced as an administrative measure that all of the information would be retained for a period of six years from collection.

The Privacy Commissioner was understandably outraged. He said: "It is contrary to the explicit written undertaking that was made by CCRA to me as an Officer of Parliament, and hence through me to Parliament, when the relevant amendments to the *Customs Act* were before Parliament." The Commissioner obtained legal opinions as to the constitutionality of the measures from three distinguished lawyers, a former Deputy Minister of Justice, a former Minister of Justice and a former Justice of the Supreme Court of Canada. (While a member of the Supreme Court of Canada, Justice La Forest wrote many of the Court's leading judgements in the area of privacy, and stated that privacy is "at the heart of liberty in a modern state.") In the opinion of each of the lawyers, the measures failed to meet constitutional requirements.

In a letter to Minister Caplan, Mr. Radwanski said:

> This is an unprecedented intrusion on the privacy rights of Canadians. It is, to the best of my knowledge, the first time the federal government has set out to build a database on all Canadians using personal information obtained from third parties without their individual consent, for purposes not of providing any service to individuals but rather of having the information available to potentially use against them.

He noted that he had been given explicit undertakings by officials of the Ministry that that data not viewed or used by a reviewing officer would be destroyed within 24 hours. On the basis of these assurances he expressed no privacy objection to the proposed amendment and did not need to avail himself of the opportunity to appear before the House of Commons and Senate committees that studied the legislation.

> Had there not been such undertakings, I would have expressed the same concerns that I am required to express now, and Parliament would have had the opportunity to consider the merits of such an intrusive initiative. As it is, Parliament approved a far more limited and vastly less privacy-invasive measure than the one that the CCRA is now preparing to launch. It is therefore my view that the creation of this massive database lacks the appropriate Parliamentary authority.[36]

In an unprecedented move, seven provincial and territorial Privacy Commissioners (including Ontario) wrote a joint letter to the Minister in November, expressing deep concern about the plan. They said that they were concerned that the database was overly broad, and targets innocent Canadians for surveillance by the state. They shared the concerns of Commissioner Radwanski that the information collected could be used for purposes unrelated to anti-terror activity. Rather than the collection of information on a small number of targeted air travellers, as originally planned, the database had now expanded significantly in scope, and the government had indicated that it might later apply to travellers arriving in Canada by train or bus.

The Commissioners were also worried about the use of this information by the police for purposes that had nothing to do with anti-terror, but for ordinary criminal law purposes. "The public interest in combating terrorism cannot be used as an excuse to expand the powers of the police or other agencies of the state, for other purposes."[37]

In a separate letter, the Ontario Commissioner wrote to the Minister about the database:

> The development of a massive system for surveillance, profiling and data mining, when applied beyond the legislated auspices of anti-terrorism, cannot be countenanced.
>
> The people of Canada do not wish to have their every activity monitored, tracked and analyzed.... If you wish to expand the general powers of law enforcement, then the public must be consulted. I respectfully suggest that the people of Canada deserve to have an open debate over any substantial expansion of powers beyond the original purpose of combating terrorism.[38]

The submissions of the Commissioners met with some success. On April 9, 2003, the Privacy Commissioner of Canada announced that the Minister of Revenue had written to him about changes to the traveller database program that "very substantially address the concerns expressed by myself and many others." The Commissioner published the Minister's letter, in which she said that she had given due consideration to the privacy concerns that had been raised. The Commissioner summarised the changes to the program as follows:

- Advance Passenger Information (API) – which consists only of passport information such as name and date of birth and does not include any specific travel information – will continue to be stored for six years and can be widely shared under Section 107 of the *Customs Act*.

- The much more detailed Passenger Name Record (PNR) – which contains all the information held by an airline – will immediately be purged by the CCRA of all meal and health information.

- PNR data will still be held for six years, but use and access will vary by length of retention, which is divided into three time periods.
- For the first 72 hours, it will be used by customs and immigration officers to assess risk, as at present.
- From 72 hours to two years, the information will be depersonalized and used, without names attached, only by intelligence officers and analysts. The information can be re-identified with the traveller's name only when necessary for customs purposes.
- During this two-year period, information will only be shared with other agencies or departments for non-customs purposes if a warrant has been obtained. This includes the tax side of the CCRA.
- Where information relates to a customs offence, the CCRA will disclose it to law enforcement authorities on its own initiative. It will share information with other countries, to assist with a customs investigation, in accordance with written agreements.
- From two years to six years, the information can only be used to fulfill the CCRA's mandate regarding the security of Canada, rather than all customs purposes. It will be used on a depersonalized basis unless the Commissioner of the CCRA personally approves re-personalizing it based on reason to suspect that the name or other identifying elements are necessary to deal with a high-risk person.
- During this final period, information can only be shared with agencies that have a national security or defence mandate, where there are reasonable grounds to believe that the information relates to a real or apprehended threat.

The Commissioner described the effect of the changes as moving "from an open-ended, unrestricted intrusion on privacy into a much more nuanced, restrained and appropriate instrument."[39]

European Union

Video Surveillance Consultation

Video surveillance by closed circuit television cameras has become ubiquitous in public places. The proliferation of the cameras has raised concerns about the continuous surveillance of citizens throughout the European Union. As a response, the European Commission has begun a public consultation, which will lead to a working paper on "the Processing of Personal Data by means of Video Surveillance." The working paper is intended to contribute to the uniform application of the national measures adopted under Directive 95/46/EC dealing with video surveillance. The paper will examine conditions and limitations on the use of video-surveillance, and the necessary safeguards for citizens. The Commission will receive comments until May 31, 2003.

The European Data Protection Commissioners may adopt a recommendation on this question.[40]

Passenger Name Record (PNR) Transmission to US Customs

In February 2003, and the Commission of the European Union issued a Joint Statement with the United States to permit EU airlines to provide to the US authorities, data on EU passengers, including access to the reservation databases of the airlines.

The US represented to the EU Commission that "by legal statute (title 49, United States Code, section 44909(c)(3)) and its implementing (interim) regulations (title 19, Code of Federal Regulations, section 122.49b), air carriers operating passenger flights in foreign air transportation to, from or through the United States, must provide Customs with electronic access to PNR data contained in the automated reservation/ departure control systems ('reservation systems')." The required information could have been collected from passenger tickets and other passenger documents upon arrival, but it was stated that this would cause too many delays.

As was stated in an opinion dated October 24, 2002 of the EU Working Party under Article 25 of the EU Data Protection Directive:

> Airlines find themselves caught in a dilemma in that although, on the one hand, they are obliged to observe the legislation on data protection transposing Directive 95/46/EC, on the other hand US legislation obliges airlines to forward data and is backed up by severe penalties.

In its opinion, the Working Party considered the collection to be for a purpose other than that for which it had been collected by the airlines an travel agents, and excessive as to the amount of personal information being collected (especially that contained in the airlines reservations systems). Further, it was a transmission to a third country where there were concerns about the adequacy of the levels of privacy protections that would be offered. Each of these elements would lead to a breach of the Directive.[41]

The Joint Statement was an attempt to find a resolution for the problems raised by Passenger Name Record (PNR) transmission requirements contained in the *Aviation and Transportation Security Act 2001*. The joint statement says: "It was necessary in particular to reconcile US requirements with the requirements of data protection law in the EU."

The agreement involves the processing of PNR data for persons whose current travel itinerary includes flights into, out of, or through the US. The data relates to both passengers and crew and must be transmitted electronically, and sent before the plane takes off. It was hoped that compliance with the agreement would not result in action being taken under Article 25 of the EU Privacy Directive against complying airlines.

In the Joint Statement, the US agreed to respect the principles of the EU Data Protection Directive and to develop measures to protect sensitive personal information. Data subjects can apply to US Customs for access to their own personal information through FOIA. The agreement provides for disclosure of the PNR to US authorities for purposes that go beyond national security and the war against terrorism:

> US Customs may provide information to other US law enforcement authorities only for purposes of preventing and combating terrorism and other serious criminal offences, who specifically request PNR information from US Customs. (clause 5e.)[42]

The agreement was controversial in the European Union for a variety of reasons, not least of which was that the process for arriving at an agreement had been truncated. The Chair of the EU Working Party Stephano Rodota, requested that the Joint Statement be postponed, "for as long as required in order to finalise a quick formal procedure." In a letter dated March 3, 2003 to the chair of the European Parliament's Committee on Citizens' Freedoms and Rights, Mr. Rodota said that, "many delegations" attending the meeting of the Council of the European Union's Working Party on Aviation on 20 February raised "doubts and concerns in respect of the legal nature, contents or actual force of the Joint Statement." He says that the factual circumstances, of the Joint Statement which allows US Customs to directly access the reservation databases of airlines based in the EU is "devoid of a legal base."

He said that the agreement could give rise to complaints to Data Protection Authorities on a national basis by individuals who are aggrieved by the data transmission.[43]

Retention of Electronic Communications Traffic Data

The European Data Protection Commissioners have noted with concern that proposals are being considered, which would result in the mandatory, systematic retention of traffic data concerning all kinds of telecommunication (i.e. details about time, place and numbers used for phone, fax, e-mail and other use of the internet) for a period of one year or more, in order to permit possible access by law enforcement and security bodies.

The Data Protection Commissioners expressed grave doubts as to the legitimacy and legality of the proposals. They also noted the excessive costs that would have to be borne by the telecommunications industry. The Commissioners were of the view that "such retention would be an improper invasion of the fundamental rights guaranteed to individuals by Article 8 of the European Convention on Human Rights, as further elaborated by the European Court of Human Rights. (see Opinion 4/2001 of the Article 29 Working Party established by Directive 95/46/EC, and Declaration of Stockholm, April 2000)."

The Commissioners requested to be consulted on measures that are proposed, before they are adopted.[44]

According to Statewatch, a civil liberties organization tracking developments, although there is not at the present a move to push through an EU Directive requiring the retention by member states of communications traffic data, such data is being retained by national member states under their domestic law. Statewatch obtained a copy of Room Document No. 7, which set out the results of a country-by-country survey of retention law and practice. (Statewatch is appealing a decision of the Council of the European Union refusing access to document, on the grounds that it would reveal national weaknesses and vulnerabilities in this area.)

On the basis of the survey, Statewatch concluded:

1. Nine of the 15 EU states have or intend to introduce an obligation for the retention of data, two member states have no plans and four are unclear.

2. The norm for the period of data retention would appear to be 12 months, although Ireland is way out ahead with 3 years.

3. Ten of the 15 EU states would support a EU measure, only two are against this and three are unclear.[45]

Privacy in Japan

In a move away from self-regulation of privacy protection by private sector entities, the Japanese government has been mooting a privacy bill for some years. On April 8, 2003, debate began in the House on a set of government bills designed as a framework for both governmental and commercial usage of personal information.

The government bills have occasioned a great deal of controversy. A similar bill was scrapped last year because it was feared that it would unduly restrict freedom of the press. Revisions to the bill omitted the "five principles" including the specification of the purpose for the collection of personal information. Under the new bills, the government can use the personal information for other than its original purpose for legitimate reasons. Fines and imprisonment can result for government official offenders who improperly disclose personal information.

The four Opposition parties introduced their own privacy bill on April 4, 2003. The Opposition bill would prohibit the collection of sensitive personal information. This is defined as political or religious inclination or beliefs. Special care should be taken in handling personal information such as medical records, welfare payment records, criminal records, any information on race, ethnicity or social status. This type of information can be used in a discriminatory way, and its collection should be prohibited unless to save the individual's life. The bill would also give the individual control over his personal information, including a right of correction, and a right to block disclosure.

The government bill does not define sensitive personal information, nor does it make it subject to special controls.

The Opposition bill would provide for an independent legislative committee to deal with complaints, whereas the government model would have oversight by a relevant minister. The press is somewhat concerned that the Opposition bill would not sufficiently protect freedom of the press.

On May 23, 2003, the set of five privacy protection bills were approved by the Upper House of Parliament.

Privacy in Australia

It has been reported that the Government of Australia is maintaining a list of individuals whom it wishes to bar from the country. It has been described as a "blacklist" containing about 250,000 names, with their known aliases. The list is known as the "Movement Alert List," and the individuals on the list may be suspected of being terrorists, may owe money to the government, or be of "health concern." A person seeking entry whose name appears on the list might be denied a visa. Australia has a universal visa requirement.[46]

Three universities have tried to find ways around federal court orders obtained by the music industry that would permit the record companies to search all university computers for evidence of music piracy.

The Universities of Melbourne, Tasmania and Sydney have engaged the Australian Vice-Chancellors' Committee to negotiate consent orders on their behalf with the record companies. The universities want to know what specific information the record companies are looking for, as part of negotiating terms of access.[47]

On another front, the government of New South Wales is considering legislation to ban the use of video surveillance cameras (or "kiddy cams") in day care centres. The cameras have become quite ubiquitous, and permit parents to see their children and surroundings on the Internet. They are opposed by teachers who object to being surveilled while at work, and by privacy advocates who say that images of other children can be accessed by the parents. The Department of Community Services fears that the images of the children could be accessed by pedophiles.[48]

In another workplace story, the Victorian Law Reform Commission has decided to study privacy issues in the workplace, and will publish a paper on the topic. With the increase in the use of workplace monitoring technology, the Commission Chair said that it was time to decide what practices were appropriate. The issues to be studied include drug testing, e-mail monitoring and the use of biometrics such as retinal scanning and fingerprinting. Employees are becoming increasingly concerned about the level of monitoring, and Privacy Commissioner Malcolm Crompton said that it was important that employees have notice of surveillance.[49]

Conclusion

This brief survey of some of the developments in the privacy arena during the past year demonstrates that those who are concerned with the maintenance of our traditional liberties must not relax their vigilance.

Where reasoned opposition has been voiced to government initiatives, there have been some positive results where governments responded by scaling back programs to more nuanced and targeted models. Examples which have not been discussed in this paper include a decision by the government of the Philippines not to move forward with a national ID card, and a decision by the UK government to scale back plans to permit wholesale government access to telephone, Internet and e-mail records.

Similarly the Canadian bar has been successful in persuading the government that requiring lawyers to report on their clients is an untenable derogation from solicitor and client privilege. It also appears that the US Securities and Exchange Commission is prepared to listen to those concerns, and to consult with the bar in the attempt to find a solution.

The importance of privacy as the underpinning for other rights and freedoms has been underscored by the broad-based range of individuals and organizations that have felt it important to make submissions to government on these issues and let their views be known.

These successes are encouraging, but much remains to be done.

Notes

1. The *Personal Information Protection and Electronic Documents Act* (PIPEDA) S.C. 2000 c.5, <www.parl.gc.ca/36/2/parlbus/chambus/house/bills/government/C-6/C-6_4/C-6_cover-E.html>.

2. The Commissioner's summaries are to be found on his Web site, <www.privcom.gc.ca/cf-dc/2003/index2-3_e.asp>.

3. *PIPED Act* Case Summary #42: Air Canada allows 1% of Aeroplan membership to "opt out" of information sharing practices, March 11, 2002, <www.privcom.gc.ca/cf-dc/cf-dc_020320_e.asp>.

4. *PIPED Act* Case Summary #35: Bank customer objects to being surveyed by private firm, January 10, 2002, <www.privcom.gc.ca/cf-dc/cf-dc_020110_02_e.asp>.

5. *PIPED Act* Case Summary #124: Individual complains of delayed response to credit history request and refusal to amend personal information, March 4, 2003, <www.privcom.gc.ca/cf-dc/2003/cf-dc_030303_e.asp>.

6. Application of the *Competition Act* to Representations on the Internet, Industry Canada, <strategis.ic.gc.ca/SSG/ct02500e.html>.

7. Letter from Privacy Commissioner to Minister of Justice, March 7, 2003, <www.privcom.gc.ca/media/nr-c/2003/02_05_b_030307_e.asp>.

8. *Smith v. Jones* [1999] 1 S.C.R. 455.

9. *Lavallee, Rackel & Heintz v. Canada (Attorney General)*[2002] 200 SCC 61.

10. *City of Montreal v. La Societe d'energie Foster Wheeler Ltee* (Que.) SCC (28967).

11. *The Proceeds of Crime (Money Laundering) and Terrorist Financing Act* S.C. 2001.

12. The provincial law societies are the governing bodies for the legal profession in Canada.

13. CBA welcomes government retreat on Money Laundering Act, <www.cba.org/CBA/News/2003_Releases/2003-04-01_laundering.asp>.

14. CBA Says New U.S. SEC Rules a Threat to Canadians and their Lawyers, <www.cba.org/CBA/News/2002_Releases/sec.asp>.

15. SEC Adopts Attorney Conduct Rule Under Sarbanes-Oxley Act, <www.sec.gov/news/press/2003-13.htm>.

16. CBA Calls New U.S. Securities and Exchange Commission Proposals a Positive Step, <www.cba.org/CBA/News/2003_Releases/sox.asp>.

17. Commissioner's letter to the Premier regarding the failure to introduce legislation, December 16, 2002, <www.ipc.on.ca/scripts/index_.asp?action=31&P_ID=13718&N_ID=1&PT_ID=11457&U_ID=0>.

18. Release of patient's personal records a wake-up call to all companies: Cavoukian, February 20, 2003, <www.ipc.on.ca/scripts/index_.asp?action=31&P_ID=14075&N_ID=1&PT_ID=13169&U_ID=0>.

19. Privacy Commissioner Ann Cavoukian announces joint research program with the Ponemon Institute to compare Canadian and American corporate privacy, January 27, 2003, <www.ipc.on.ca/scripts/index_.asp?action=31&P_ID=13994&N_ID=1&PT_ID=13169&U_ID=0>.

20. Private Sector Privacy Consultations 2002, Government of British Columbia, June 2002, <www.mser.gov.bc.ca/foi_pop/psp/pspcon2002.htm>.

21. *Haskett v. Equifax*, docket C37573 & C37574, Court of Appeal for Ontario, March 6, 2003.

22. Order H2002-003, Information and Privacy Commissioner of Alberta, March 19, 2003, <www.oipc.ab.ca/ims/client/upload/H2002-003.pdf>.

23. *PIPED Act* Case Summary #14: Selling of information on physicians' prescribing patterns, September 21, 2001, <www.privcom.gc.ca/cf-dc/cf-dc_010921_e.asp>.

24. *Blackburn v. Midland Walwyn Capital Inc.*[2003] O.J. No. 621 OntSupCtJus - 2003 Jan 22.

25. <www.privcom.gc.ca/media/nr-c/2003/02_05_b_030129_e.asp>.

26. Commissioner Ann Cavoukian shares the federal Privacy Commissioner's concerns over Ottawa's data-grab under the guise of anti-terrorism, January 30, 2003, <www.ipc.on.ca/scripts/index_.asp?action=31&P_ID=14024&N_ID=1&PT_ID=13169&U_ID=0>.

27. Privacy Commissioner's Annual Report: George Radwanski's Concerns Justified Says Civil Liberties Coalition, International Civil Liberties Monitoring Group, January 30, 2003, <www.privcom.gc.ca/media/le_030131_e.asp>.

28. <www.canada.justice.gc.ca/en/cons/la_al/law_access.pdf>.

29. Lawful Access – Consultation Document, Department of Justice, August 25, 2002, <canada.justice.gc.ca/en/cons/la_al/>.

30. A letter from Commissioner Ann Cavoukian to Martin Cauchon, Minister of Justice and the Attorney General of Canada, outlining her concerns about the "Lawful Access" proposals, December 10, 2002, <www.ipc.on.ca/scripts/index_.asp?action=31&P_ID=13724&N_ID=1&PT_ID=11457&U_ID=0>.

31. Comments on *Lawful Access – Consultation Document* (August 25, 2002) – OIPC File No. 16763, David Loukidelis, Information and Privacy Commissioner of British Columbia, December 16, 2002, <www.oipc.bc.ca/new/16763-ISP.pdf>.

32. Statement before the House of Commons Standing Committee on Citizenship and Immigration regarding a national identity card, Privacy Commissioner of Canada, March 18, 2003, <www.privcom.gc.ca/speech/2003/02_05_a_030318_e.asp>.

33. *Customs Act* R. S.C. 1985 c.1.

34. *Bill S-23, An Act to Amend the Customs Act and related amendments to other acts*, passed October 25, 2001.

35. s. 3 *Passenger Information (Customs) Regulation* under the *Customs Act* The Regulation came into force on the date that it was published – October 4, 2002.

36. Letter to the Honourable Elinor Caplan, Minister of National Revenue with legal opinions from retired Supreme Court Justice Hon. Gérard V. La Forest, C.C., Q.C. and from Mr. Roger Tassé, O.C., Q.C. from the Privacy Commissioner of Canada, November 22, 2003, <www.privcom.gc.ca/media/nr-c/02_05_b_021122_e.asp>.

Letter to the Hon. Elinor Caplan, Minister of National Revenue, from the Privacy Commissioner of Canada, December 18, 2002, <www.privcom.gc.ca/media/nr-c/02_05_b_021218_e.asp>.

Letter to the Hon. Elinor Caplan, Minister of National Revenue from the Privacy Commissioner of Canada, January 9, 2003, <www.privcom.gc.ca/media/nr-c/2003/02_05_b_030109_e.asp>.

37. Letter from 7 provincial Privacy Commissioners to the Hon. Elinor Caplan, November 22, 2002, <www.ipc.on.ca/userfiles/page_attachments/111202-let.pdf>.

38. A letter from Commissioner Ann Cavoukian to the Honourable Elinor Caplan, Minister of Revenue, regarding the Canada Customs and Revenue Agency's traveller-surveillance database, November 20, 2002, <www.ipc.on.ca/scripts/index_.asp?action=31&P_ID=13752&N_ID=1&PT_ID=11457&U_ID=0>.

39. Letter of Elinor Caplan, Minister of Revenue to the Privacy Commissioner of Canada, April 8, 2003, <www.privcom.gc.ca/media/nr-c/2003/02_05_b_030408_e.asp>.

40. Notice of Consultation and working document, <europa.eu.int/comm/internal_market/en/dataprot/wpdocs/consultation_en.htm>.

Working Document on the Processing of Personal Data by means of Video Surveillance, <europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2002/wp67_en.pdf>.

41. *Opinion 6/2002 on transmission of Passenger Manifest Information and other data from Airlines to the United States*, Working Party on the Protection of Individuals With Regard to the Processing of Personal Data, <europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2002/wp66_en.pdf>.

42. Joint Statement, <www.statewatch.org/news/2003/feb/11usdata2.htm>.

43. <www.statewatch.org/news/2003/mar/02usdata.htm>.

44. Opinion 5/2002 on the Statement of the European Data Protection Commissioners at the International Conference in Cardiff (9-11 September 2002) on mandatory systematic retention of telecommunication traffic data; Adopted on 11 October 2002, <europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2002/wp64_en.pdf>.

45. Majority of governments introducing data retention of communications, Statewatch, January 12, 2003, <www.statewatch.org/news/2003/jan/12eudatret.htm>.

46. Alert list grows fat with names of terrorism, Sydney Morning Herald., March 10, 2003, <www.smh.com.au/articles/2003/03/09/1047144872489.html>.

47. Digging for pirates' gold, The Age (Australia), March 25, 2003, <www.theage.com.au/articles/2003/03/24/1048354520508.html>.

48. Ban on 'kindycam' at centres, The Age (Australia), March 22, 2003, <www.theage.com.au/articles/2003/03/21/1047749940264.html>.

49. <www.theage.com.au/articles/2003/03/22/1047749989637.html>.

Information and Privacy Commissioner/Ontario

80 Bloor Street West
Suite 1700
Toronto, Ontario
M5S 2V1

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Web site: www.ipc.on.ca